Appalachian School of Law
Information Security Program

Policy Statement

The Appalachian School of Law (ASL) Information Security Program (ISP) is intended as a set of comprehensive guidelines and policies designed to safeguard all sensitive data maintained at the Law School and to comply with applicable laws and regulations on the protection of Personal Information, as that term is defined below, found on records and in systems owned by the School.

1. Overview

The ISP was implemented to comply with regulations set forth by federal and Virginia state laws. ASL is required to take measures to safeguard personally identifiable information, including financial information, and to provide notice about security breaches of protected information at the Law School to affected individuals and appropriate state agencies.

In addition, ASL is committed to protecting the confidentiality of all sensitive data that it maintains, including information about individuals who work or study at the Law School. ASL has implemented a number of policies to protect such information, and the ISP should be read in conjunction with these policies.

ASL's Director of Information Services is designated as the Qualified Individual (QI) and is responsible for the implementation and supervision of the program.

2. Purpose

The purposes of this document are to:

- Establish a comprehensive information security program with policies designed to safeguard sensitive data that is maintained by the Law School, in compliance with federal and state laws and regulations;
- Establish employee responsibilities in safeguarding data according to its classification level; and
- Establish administrative, technical, and physical safeguards to ensure the security of sensitive data.

3. Scope

This Program applies to all ASL employees, whether full- or part-time, including faculty, administrative staff, union staff, contract, and temporary workers, hired consultants, interns, and student employees, as well as to all other members of the ASL community (hereafter referred to as the "Community"). The data covered by this Program includes any information stored, accessed, or collected at the Law School or for Law School operations. The ISP is not intended to supersede any existing ASL policy that contains more specific requirements for safeguarding certain types of data, except in the case of Personal Information and Nonpublic Financial Information, as defined below. If such a policy exists and is in conflict with the requirements of the ISP, the other policy takes precedence.

3.1. Definitions

Personal Information (PI)

Personal Information (PI) is the first name and last name or first initial and last name of a person in combination with any one or more of the following:

- Social Security number;
- Driver's license number or state-issued identification card number; or
- Financial account number (e.g., bank account) or credit or debit card number that would permit access to a person's financial account, with or without any required security code, access code, personal identification number, or password.

For the purposes of this Program, PI also includes passport number, alien registration number, or other government-issued identification numbers.

Nonpublic Financial Information

The GLB Act (FTC 16 CFR Part 313) requires the protection of "customer information", that applies to any record containing nonpublic financial information ("NFI") about a student or other third party who has a relationship with the Law School, whether in paper, electronic or other forms, which is handled or maintained by or on behalf of the Law School. For these purposes, NFI shall include the information:

- A student or other third party provides in order to obtain a financial product or service from the Law School;
- About a student or other third party resulting from any transaction with the Law School involving a financial product or service; or
- Otherwise obtained about a student or other third party in connection with providing a financial product or service to that person.

Examples of NFI include:

- Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;
- Account balance information, payment history, overdraft history, and credit or debit card purchase information;
- The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;
- Any information about your consumer, if it is disclosed in a manner that indicates that the individual is or has been your consumer;

- Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;
- Any information you collect through an Internet “cookie” (an information collecting device from a web server), and
- Information from a consumer report.

3.2. Data Classification

All data covered by this policy will be classified into one of three categories outlined below, based on the level of security required for each, starting with the highest level.

Confidential

Confidential data refers to any data where unauthorized access, use, alteration, or disclosure of this data could present a significant level of risk to ASL or the Community. Confidential data should be treated with the highest level of security to ensure the privacy of that data and prevent any unauthorized access, use, alteration, or disclosure.

Confidential data includes any data that is protected by federal or state laws or regulations, including, but not limited to, data protected under the following privacy laws: Health Insurance Portability and Accountability Act of 1996 (HIPAA), Family Educational Rights and Privacy Act (FERPA), 16 CFR 313 (Privacy of Consumer Financial Information), the Federal Gramm-Leach-Bliley Act, and the FTC’s Red Flag Rules. Information protected by these laws includes, but is not limited to, PI, NFI, Protected Health Information (PHI), student education records, and financial aid information.
Confidential data also includes other sensitive personal and institutional data where the loss of such data could harm an individual’s right to privacy or negatively impact the finances, operations, or reputation of ASL. This data includes, but is not limited to, donor information, intellectual property, School financial and investment records, employee salary information, or information related to legal or disciplinary matters.

Internal Use Only

Internal Use Only data refers to any data where unauthorized access, use, alteration, or disclosure of this data could present a moderate level of risk to ASL. This data should be limited to access by individuals who are employed by or matriculate at ASL and who have legitimate reasons for accessing such data. Any nonpublic data that is not explicitly designated as Confidential should be treated as Internal Use Only data. A reasonable level of security should be

applied to this classification to ensure the privacy and integrity of this data.

Public (or Unrestricted)

Public data includes any information for which there is no restriction to its distribution, and where the loss or public use of such data would not present any harm to ASL or members of the ASL community. Any data that is not classified as Confidential or Internal Use Only should be considered Public data.

4. Policy

4.1. Responsibilities

All data at the Law School is assigned a data owner according to the constituency it represents. Data owners are responsible for the approval of all requests for access to such data. The data owners for each constituency group are designated as follows:

- Faculty data - the Dean (or his or her designee) serves as the data owner
- Staff data - the Director of Community Service and Personnel (or his or her designee) serves as the data owner
- Student data – Shared between the Registrar, Dean of Admissions, Financial Aid Officer, and Director of the Business Office (or his or her designees)
- Alumni Data – Director of Alumni Relations (or his or her designee)
- Financial & Accounting Data – Business Office Director and CFO

Information Services (IS) staff serve as the data stewards for all data stored centrally on the Law School's servers and administrative systems and are responsible for the security of such data. For distributed data stored on departmental servers, the department head or their designee serves as the data steward, and IS and the department share joint responsibility for securing the data.

Personnel will inform IS staff about an employee's change of status or termination as soon as is practicable, but before an employee's departure date from the Law School. Changes in status may include terminations, leaves of absence, significant changes in position responsibilities, transfer to another department, or any other change that might affect an employee's access to Law School data. IS staff will terminate all of the employee's account access upon the employee's termination date from the Law School, as specified by Personnel.

Department heads will alert IS at the conclusion of a contract for individuals who

are not considered ASL employees in order to terminate access to their ASL accounts. The Information Services Department is in charge of maintaining, updating, and implementing this Program. All members of the Community are responsible for maintaining the privacy and integrity of all sensitive data as defined above, and must protect the data from unauthorized use, access, disclosure, or alteration. All members of the Community are required to access, store, and maintain records containing sensitive data in compliance with this Program.

4.2. Identification and Assessment of Risks to School Information

ASL recognizes that it has both internal and external risks to the privacy and integrity of Law School information. These risks include, but are not limited to:

- Unauthorized access to Confidential data by someone other than the owner of such data
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access to Confidential data by employees
- Unauthorized requests for Confidential data
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of Confidential data through third parties

ASL recognizes that this may not be a complete list of the risks associated with the protection of Confidential data. Since technological growth is not static, new risks are created regularly. Accordingly, IS will actively participate and monitor advisory groups such as the Educause Security Institute, the Internet2 Security Working Group, and SANS for the identification of new risks.

The Information Services Department also performs periodic risk assessments. These may include:

- Security evaluations of safeguards,
- Inventory of data storage and transmission,
- Risk and compliance assessment,
- Data recovery and contingency planning, and
- Review of policies and procedures.

4.3. Policies for Safeguarding Confidential Data

To protect Confidential data, the following policies and procedures have been developed that relate to protection, access, storage, transportation, and destruction of records, computer system safeguards, and training.

Access

- Only those employees or authorized third parties requiring access to Confidential data in the regular course of their duties are granted access to Confidential data, including both physical and electronic records.
- Computer and network access passwords are disabled upon the termination of employment or relationship with ASL.
- Upon termination of employment or relationship with ASL, physical access to documents or other resources containing Confidential data is immediately prevented.

Storage

- Members of the Community will not store Confidential data anywhere other than secure devices or locations as authorized by the Information Services Department.
- To the extent possible, making sure that all Confidential data is stored only on secure servers maintained by the Law School and not on local machines, unsecure servers, or portable devices.
- Paper records containing Confidential data must be kept in locked files or other secure areas when not in use.
- Electronic records containing Confidential data must be stored on secure servers, and, when stored on authorized desktop computers, must be password-protected.

  Confidential data must not be stored on cloud-based storage solutions that are unsupported by the Law School (including Dropbox, Microsoft OneDrive, Apple iCloud, etc.).

Removing Records from Campus

- Members of the Community are strongly discouraged from removing records containing Confidential data off-campus. In rare cases where it is necessary to do so, the user must take all reasonable precautions to safeguard the data. Under no circumstances are documents, electronic devices, or digital media containing Confidential data to be left unattended in any insecure location.
- When there is a legitimate need to provide records containing Confidential data to a third party, electronic records shall be password-protected

and/or encrypted, and paper records shall be marked confidential and securely sealed.

Traveling Abroad with Students' Personal Information

- In the event that transmission of student passport information is required by the hotel or program abroad in advance of the travel, only the relevant information requested (e.g., Name, Passport Number, Date of Expiry, and Date of Birth) will be provided, not complete copies of the passport images. This information should first be transmitted via Fax, provided that the ASL department arranging the travel confirms the accuracy of the Fax number by sending an initial confirmation message before the actual data. If Faxing is unavailable, the data may be sent securely via email (using the SSL version of Google Mail), provided that the same confirmation of transmission takes place.
- Faculty/staff who need to retain these passport numbers for arranging travel will store this data in spreadsheets that are saved on the Law School's secure storage servers. Any spreadsheets containing student passport information will be routinely deleted when not needed.
- Faculty/staff who are traveling with the students abroad that need student passport and visa information for hotel check-in will keep a paper record on their person that contains relevant information (such as the passport and visa numbers and their expiration dates) and the last names of the students only. Faculty/staff must not retain or travel with copies of student passports.
- In extreme circumstances involving travel to a remote location where access to technology would be limited and would prohibit the retrieval of a lost passport, a program director may request an exemption to this policy, allowing for him or her to retain copies of the students' passports during travel. This request will be made to the Director of Information Services for approval. If the request is approved, the program director will sign the "Faculty/Staff Agreement for Traveling with Secure Data" to acknowledge their understanding of the ISP and their responsibilities in protecting the passports. The program director also agrees to alert IS immediately if the copies of passports are lost.

Destruction of Confidential Data

- Records containing Confidential data must be destroyed once they are no longer needed for business purposes unless state or federal regulations require maintaining these records for a prescribed period of time.
- Paper and electronic records containing confidential data must be destroyed in a manner that prevents the recovery of the data.

Third-Party Vendor Agreements Concerning Protection of Personal Information

ASL exercises appropriate diligence in selecting service providers capable of maintaining appropriate security safeguards for PI provided by the Law School to them. The primary budget holder for each department is responsible for identifying those third parties providing services to the Law School that have access to PI. All relevant contracts with these third parties are reviewed and approved by the ASL Information Services Department to ensure the contracts contain the necessary language regarding safeguarding PI. It is the responsibility of the primary budget holders to confirm that the third parties are required to maintain appropriate security measures to protect PI consistent with this Program and State and Federal laws and regulations.

4.4. Policies for Safeguarding Internal Use Only Data

- Access to Internal Use Only Data should be limited to members of the Community who have a legitimate business need for the data.
- Internal Use Only Data can be stored on password-protected ASL-owned devices and services.
- Internal Use Only data may be stored on cloud-based storage solutions that are unsupported by the Law School as long as they are in compliance with the requirements of any laws governing the protection of such data (e.g., FERPA).
- Documents containing Internal Use Only Data should not be posted publicly.

4.5. Password Requirements

In order to protect College data, all members of the Community must select unique passwords following the ASL Password Construction Guidelines:

Strong passwords are long. The more characters you have, the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include "*It's time for vacation*" or "*block-curious-sunny-leaves*". Passphrases are both easy to remember and type yet meet the strength requirements. Poor or weak passwords have the following characteristics:

- Contain eight characters or less.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Are some version of "Welcome123" "Password123" "Changeme123"

In addition, every work account should have a different, unique password. Whenever possible, it is also recommended to enable the use of multi-factor authentication.

Multi-Factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource, such as an application or Website. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.

Members of the community must protect the privacy of their passwords. Passwords must not be shared with others. If an account or password is suspected to have been compromised, all passwords should be changed immediately and the incident reported to the Information Services Department.

4.6. Computer System Safeguards

The IS staff monitors and assesses information safeguards on an ongoing basis to determine when enhancements are required. The Law School has implemented the following to combat external risk and secure the Law School's network and data containing Confidential information:

- Secure user authentication protocols:
    - Unique passwords are required for all user accounts; each employee receives an individual user account.
    - Server accounts are locked after multiple unsuccessful password attempts.
    - Computer access passwords are disabled upon an employee's termination.
    - User passwords are stored in an encrypted format; root passwords are only accessible by system administrators.
- Secure access control measures:
    - Access to specific files or databases containing Confidential Information is limited to those employees who require such access in the normal course of their duties.
    - Each such employee has been assigned a unique password, different from the employee's password to the computer network, to obtain access to any file or database that contains Confidential Data needed by the employee in the course of his or her duties.
    - Files containing Confidential Data transmitted outside of the ASL network are to be encrypted.
    - Maintain an appropriate internal audit, which records system activity such as log-ins, file accesses, and security incidents

- The IS Department performs regular internal network security audits of all server and computer system logs to discover, to the extent reasonably feasible possible electronic security breaches, and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Data.
- All School-owned computers and servers are firewall-protected and regularly monitored.
- Operating system patches and security updates are installed on all servers on a regular basis.
- Antivirus and anti-malware software are installed and kept updated on all servers and workstations.

4.7. Service Providers

ASL ensures service providers implement and maintain appropriate safeguards with respect to private information. Information Services reviews vendors to ensure their products and services are compatible with ASL's information technology and security principles. Information Services also works with the General Counsel, as appropriate, to ensure that service provider contracts contain appropriate terms to protect the security of confidential data.

4.8. Application Development and Security

- Ensure conformance with all appropriate security requirements,
- Protect sensitive information throughout its life cycle,
- Facilitate efficient implementation of security controls,
- Prevent the introduction of new risks when modified,
- Ensure proper removal of data when the system is retired.

Application software must be tested before installation in a production environment, and be protected from unauthorized changes. Application updates must be applied in a timely manner, commensurate with the risk associated with the addressed vulnerability.

4.9. Change Control

Change control management must be implemented for systems handling non-public institutional data, to monitor and control hardware and software configuration changes. Change control includes documentation of change requests, approvals, testing, and final implementation. Change control management is required for both physical hardware as well as cloud services.

4.10. Employee Training

All employees who access Confidential data or who otherwise have access to PI are required to complete a yearly training on data security and their responsibilities related to this Program. The training is also strongly recommended for all employees. The Information Services Department maintains records of all such training.

4.11. Reporting Attempted or Actual Breaches of Security

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of PI, or of a breach or attempted breach of the information safeguards adopted under this Program, must be reported immediately to the Information Services Department.

The Information Services Department is charged with the identification of all data security incidents where the loss, theft, unauthorized access, or other exposure of sensitive Law School data is suspected. When the Information Services Department confirms an incident involving sensitive information, the Information Services Department will convene an Incident Team, including the Information Services Department, the Dean, and heads of any affected departments, and determine appropriate actions in their response to the breach.

The Information Services Department will document all breaches and subsequent responsive actions taken. All related documentation will be stored in the Information Services Office.

4.12. Disposal

Digital storage devices that contain licensed software programs and/or institutional data must be reliably erased and/or destroyed before the device is transferred out of ASL's control, or erased before being transferred from one department or individual to another. This does not preclude the use of physical media intended specifically for the purpose of data transfer.

All computers and digital storage devices including, but not limited to desktop workstation, laptop, server, notebook, handheld computer, and hard drives; and all external data storage devices such as disks, SANs, optical media (e.g., DVD, CD), magnetic media (e.g., tapes, diskettes), and non-volatile electronic media (e.g., memory sticks), are covered under these requirements for disposal.

5. Enforcement

Any employee or student, who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises data classified as Confidential or Internal Use Only without authorization, or who fails to comply with this Program in any other respect, will be subject to disciplinary action, which may include termination in the case of employees and expulsion in the case of students.

6. Effective date

This Written Information Security Program was implemented on December 11, 2020. ASL will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.